SA 3.2 System Administration Functional Requirements

The goal is to provide a single screen for the system administrator to access a hierarchical set of control-display interfaces.

SA 3.2.1 Each segment shall put its control-display invocation entry point into a standard subdirectory within the segment's directory structure.

Traceability:
Priority ???

SA 3.2.2 It shall be able to respond to the System Administration segment's generic invocation mechanism.

Traceability:
Priority ???

SA 3.2.3 All GCCS segments, including but not limited to, the GCCS COE, ORACLE, and all applications, shall have a system administration capability which fits into the hierarchy.

Traceability:
Priority ???

SA 3.2.4 To reduce ambiguity for the system administrator, the user interface shall be heavily word oriented. A pure icon approach is too likely to slow down / increase error probabilities of a literate administrator.

Traceability:
Priority ???

SA 3.2.5 The documentation for system commands, to the extent possible, executed to perform any system administration operation shall be available on-line in human readable and modifiable form. System administration personnel must know what and how a given action is being performed, and be able to adapt it to site/crisis-peculiar circumstances. A "no looking under the hood" solution is a worthy goal, but the current state-of-the-art precludes success at this time.

Traceability:
Priority ???

SA 3.2.6 The system administration controls and displays shall permit:

- Locking and unlocking an application with an appropriate message displayed to users

  Traceability:
  Priority ???

- Determining the status of the application for a functional user

  Traceability:
  Priority ???

- Determining the status of the aspects of other segments, including the GCCS COE, which could cause a "down" state for the application

  Traceability:
  Priority ???

- Crash diagnosis and recovery

  Traceability:
  Priority ???

- Determining the version of the application and its components including any patches

  Traceability:
  Priority ???

SA 3.2.7 If relevant to a given segment, the system administration controls shall provide a way to:

- Backup and restore data associated with the application

  Traceability:
  Priority ???

- Configure the application for typically requested changes associated with the application such as user accounts

  Traceability:
  Priority ???

SA 3.2.8 The GCCS COE segment's system administration shall provide an ability to:

- Install/Deinstall software and patches

  Traceability:
  Priority ???

- Status and control of network services and operations

  Traceability:
  Priority ???

- Examine system resource utilization such as disk, cpu, and i/o

  Traceability:
  Priority ???

- Perform printer monitoring and administration

  Traceability:
  Priority ???

- Review system logs and configuration files

  Traceability:
  Priority ???

SA 3.2.1 Locking and unlocking an application with an appropriate message displayed to users

SA 3.2.1.1 The system administrator shall have a means to tell the application that it is functionally inoperative. The application will inform users who select it, that it is currently locked out. The intent is to let the users be informed gracefully that a given application is unavailable. This contrasts with the current approach where the user is uncertain if:

1. the application launched
2. if the application is working even if it launched
3. if anyone knows the application has a problem

Traceability:
Priority ???

SA 3.2.1.2 The system administrator shall have a means to tell the application it is functionally operative - that is - to run normally and do not put up the locked out message.

Traceability:
Priority ???

SA 3.2.2 Determining the status of the application for a functional user

SA 3.2.2.1 The system administrator shall have a means to determine if an application is functionally usable. The intent is to provide the administrator with a way of knowing if the application will generally work as intended for a functional user from a GCCS COE systems perspective. It is not intended to

determine if a given functional user has all the requirements he has for a given app implemented within the software.

Traceability:
Priority ???

SA 3.2.3 Determining the status of the aspects of other segments, including the GCCS COE, which could cause a "down" state for the application

SA 3.2.3.1 The system administrator shall have a means to determine if the reason an application is not functionally usable is due to the application itself or some resource the application is dependent on. For instance, an app which uses Oracle should be able to point the finger at Oracle, if it determines that Oracle is its problem. The administrator can then go to the Oracle functional usability page to get an idea about what is wrong with Oracle.

Traceability:
Priority ???

SA 3.2.4 Crash diagnosis and recovery

SA 3.2.4.1 The system administrator shall have a means to determine the cause of a crash and a recovery strategy for each application. While a total solution is not possible with the current state-of-the-art, the intent is for an application to provide a mechanism to get the same information after a crash that an application specialist could get, and recover from the crash as well as an application specialist could do. The intent is encode some of the specialist's knowledge for the benefit of the GCCS community.

Traceability:
Priority ???

SA 3.2.5 Determining the version of the application and its components including any patches

SA 3.2.5.1 The system administrator shall have a means to determine the version of the application, any patches, and relevant sub-applications. To some extent the application's version file part of the its segment holds the needed data. The rest of the data is for sub-parts of the application which are otherwise hidden at the segment level, but which are important for the administrator to know about.

Traceability:
Priority ???

SA 3.2.6 Backup and restore data associated with the application

SA 3.2.6.1 The system administrator shall have a means to backup and restore data associated with each application. The intent is for the application to provide a simple way to prompt the administrator through a tape (or other device) backup and restore of data associated with the application. If there is not sufficient data backed up to recovery an application's state, then the application's backup procedure/scripts need to be enhanced.

Traceability:
Priority ???

SA 3.2.7 Configure the application for typically requested changes associated with the application such as user accounts

SA 3.2.7.1 The system administrator shall have a means to configure the application. Most applications have a set of commonly performed customizations or changes. The system administrator should not

have to read voluminous and often out of date manuals to the needed changes. A simple user interface should prompt the administrator through commonly needed application customizations.

Traceability:
Priority ???

SA 3.2.8 Install/Deinstall software and patches

SA 3.2.8.1 The system administrator shall have a means to install and deinstall segments and patches. Effectively, the SAInstaller and associated utilities currently fulfill this requirement

Traceability:
Priority ???.

SA 3.2.9 Status and control of network services and operations

SA 3.2.9.1 The system administrator shall have a means to determine status and effect control of network services and operations for GCCS as a whole, and for individual apps as relevant. A given app may depend upon Oracle's SQL*NET; it would not be the app's requirement to check the network which SQL*NET uses unless the app found that easier to do than check to see if SQL*NET is working. Most the requirements flowing from this paragraph fall to the GCCS COE to handle.

Traceability:
Priority ???

SA 3.2.10 Requirements Submitted by the Army

SA 3.2.10.1 System Administration shall have the capability to initialize support software and pre-defined queues within 60 seconds. Start time is measured when the request is made for initialization; stop time is measured when an application program receives notification that initialization has completed.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.2 System Administration shall provide the capability to format the storage media at the request of an application program.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.3 Systema Administration shall provide the capability to maintain a workstation's on-line status in workstations that are attempting to communicate with another workstation regardless of the status of that workstaion.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.4 System Administration shall provde the capability to maintain a workstation's on-line status despite the loss of non-critical hardware devices.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.5 System Administration shall have the capability to monitor hardware configuration errors within Subsystems.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.6 System Administration shall have the capability to monitor software configuration errors.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.7 System Administration shall have the capability to monitor interface / communicastions errors with other Subsystems.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.8 System Adminstration shall have the capability to monitor software anomalies / failures during normal operations.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.9 System Administration shall have the capability to monitor memory allocation errors.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.10 System Administration shall have the capability to notify an application of any errors, anomalies, or overflow conditions.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.11 System Administration shall provide the capability for an application to review all operational diagnostics messages in the operational environment.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.12 System Administration shall have the capability to alert any application of any impending memory or disk saturation or file overwrite.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.13 System Adminstration shall provide the capability to control the following types of information during subsystem initialization:

1. Alarms for hardware malfunctions while hardware diagnostics are executing.

   Traceability: ARMY, 20 July 1996
   Priority ???

2. Alarms for software malfunctions / erros while software diagnostics are executing.

   Traceability: ARMY, 20 July 1996
   Priority ???

3. Software transitions during subsystem intialization.

   Traceability: ARMY, 20 July 1996
   Priority ???

4. Subsystem state and mode.

   Traceability: ARMY, 20 July 1996
   Priority ???

5. Access rights tables (tables for DAC and MAC checks) successfully loaded and synchronized.

   Traceability: ARMY, 20 July 1996
   Priority ???

6. Data objects in the subsystem are of the identified state type.

   Traceability: ARMY, 20 July 1996
   Priority ???

7. Control of software executing on all network workstations.

Traceability: ARMY, 20 July 1996
Priority ???

8. Control the LAN status (e.g., active, address) during and after successful LAN initialization.
Traceability: ARMY, 20 July 1996
Priority ???

9. Control of workstation logon when initialization is completed.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.14 System Administration shall have the capability to provide control which will allow initiation of the following activities:

1. Recovery from subsystem malfunctions during initialization and continuation of subsystem initialization.
Traceability: ARMY, 20 July 1996
Priority ???

2. Association of communications interfaces.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.15 System Administration shall have the capability to provide control which allows selection of the following:

1. Initiation of a cold start
Traceability: ARMY, 20 July 1996
Priority ???

2. Initiation of a warm start
Traceability: ARMY, 20 July 1996
Priority ???

3. Entry of the state/mode type (e.g., operations, exercise, training, etc.)
Traceability: ARMY, 20 July 1996
Priority ???

4. Entry of the subsystem type
Traceability: ARMY, 20 July 1996
Priority ???

5. Entry of the date and time
Traceability: ARMY, 20 July 1996
Priority ???

6. Entry of the OSRI
Traceability: ARMY, 20 July 1996
Priority ???

7. Entry of the Plain Language Address (PLA)
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.16 System Administration shall provide the capability to control the following types of information during subsystem operations:

1. Alarms for hardware malfunctions
Traceability: ARMY, 20 July 1996
Priority ???

2. Alarms for software malfunctions / errors

   Traceability: ARMY, 20 July 1996
   Priority ???

3. Users logging onto workstations

   Traceability: ARMY, 20 July 1996
   Priority ???

4. Software executing on all network workstations

   Traceability: ARMY, 20 July 1996
   Priority ???

5. LAN status (addresses, active)

   Traceability: ARMY, 20 July 1996
   Priority ???

6. Users logging off the subsystem

   Traceability: ARMY, 20 July 1996
   Priority ???

7. Workstation logon when workstation initialization is completed

   Traceability: ARMY, 20 July 1996
   Priority ???

SA 3.2.10.17 System Administration shall have the capability to provide control which will allow initiation of the following activities:

1. Recovery from malfunctions during subsytem operations and continuation without loss of state data

   Traceability: ARMY, 20 July 1996
   Priority ???

2. Assocation of communications interfaces

   Traceability: ARMY, 20 July 1996
   Priority ???

SA 3.2.10.18 System Administration shall have the capability to accept a request to add a workstation / processor (WCG or optional host processor) to the subsystem.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.19 System Administration shall have the capability to Reconfigure shared processes among the newly defined configuration of workstations within the subsystem.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.20 System Administration shall have the capability to reprioritize access to mirrored database images.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.21 System Administration shall have the capability to accept a request to delete a workstation from the subsystem.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.22 System Administration shall have the capability to accept a request to direct initialization or reconfiguration of the subsytem to permit training to take place instead of operations.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.23 Network Management Controls

SA 3.2.10.23.1 System Administration shall have the capability to:

SA 3.2.10.23.1.1 Control the operations of the network, which

1. Enable network status monitoring
   Traceability: ARMY, 20 July 1996
   Priority ???
2. Disable network status monitoring
   Traceability: ARMY, 20 July 1996
   Priority ???
3. Create a network status log
   Traceability: ARMY, 20 July 1996
   Priority ???
4. Maintain a network status log
   Traceability: ARMY, 20 July 1996
   Priority ???
5. Review network status log
   Traceability: ARMY, 20 July 1996
   Priority ???

SA 3.2.10.23.1.2 Maintain operational status informaion of selected workstations.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.23.1.3 Distribute communications network performance data between all network and workstation resources.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.23.1.4 Configure network resources utilizing CMIP (ISO DIS 9696), ...
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24 Diagnostics

SA 3.2.10.24.1 System Administration shall have the capability to monitor hardware errors upon system initialization (e.g., up until initialization is complete).
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24.2 System Administration shall have the capability to monitor software errors upon system initialization.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24.3 System Administration shall have the capability to monitor hardware configuration errors.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24.4 System Administration shall have the capability to monitor software configuration errors.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24.5 System Administration shall have the capability to monitor memory allocation errors.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24.6 System Administration shall provide the capability to log any errors to non-volatile stoarge for subsequent review.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.24.7 System Administration shall provide the capability for a new user to review all organizational diagnostic messages in the standalone environment.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.25 Normal Termination of Subsystem Operations

During normal termination, System Administration shall provide the following:

SA 3.2.10.25.1 System Administration shall initiate normal termination of a subsystem.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.25.2 System Administration shall prevent any messages from entering volatile storage areas for processing after normal termination is invoked.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.25.3 System Administration shall continue processing all volatile data (e.g., queues, buffers, transactions in progress) within the current state in an orderly manner.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.25.4 System Administration shall report that all volatile state data has been processed and the subsystem is terminated.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.25.5 System Administration shall ensure all open files are closed prior to termination of processes.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.25.6 System Administration shall ensure all processes are terminated within five(5) minutes after normal termination is invoked.
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.26 Abnormal Termination of Operations

Unplanned termination, such as power loss, can be expected and should be planned for ahead of time. System Adminstration shall provide the following:
Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.26.1 System Administration shall initiate abnormal termination.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.26.2 System Administration shall abort all images/processes on all workstations when abnormal termination is invoked.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.26.3 System Administration shall ensure all subsystem processes are terminated within one(1) minute after abnormal termination commences.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.26.4 System Administration shall provide a capability to reinitialize the subsytem (ensure workstation processes are terminated and then restart the subsytem).

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.27 Termination of Selected Analyst Processes

When an analyst is logged onto the subsystem, the system will provide a capability which does not require a workstation to have to go through a complete termination process. System Administration shall provde the following.

SA 3.2.10.27.1 System Administration shall enable an anlyst the capability to log off a workstation.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.27.2 System Administration shall ensure that the subsystem or a workstation does not require re-initialization upon analys logoff, e.g. only terminate analyst specific application processes.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.27.3 System Administration shall complete processing of all analyst specific volatile state data.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.27.4 System Administration shall allow for analyst with rights to logon after previous analyst's processes are terminated.

Traceability: ARMY, 20 July 1996
Priority ???

SA 3.2.10.28 Diagnostics Reports

The system, in concert with section Army ASIS #3.7.2.3.2, will process diagnostics on both hardware and software. The results of this will be recorded in logs for further review at the discretion of the Officer in Charge / Non-Commissioned Officer in Charge (IOC/NCOIC).

SA 3.2.10.28.1 System Administration shall provide control for review of the following diagnostic reports on-line in the operational state:

- Hardware diagnostic failures

Traceability: ARMY, 20 July 1996
Priority ???

- Hardware diagnostic status

  Traceability: ARMY, 20 July 1996
  Priority ???

- Peripheral diagnostic failures

  Traceability: ARMY, 20 July 1996
  Priority ???

- Peripheral diagnostic status

  Traceability: ARMY, 20 July 1996
  Priority ???

- Software diagnostic failures

  Traceability: ARMY, 20 July 1996
  Priority ???

- Software diagnostic status

  Traceability: ARMY, 20 July 1996
  Priority ???

SA 3.2.10.28.2 System Administration shall provide control to review the following diagnostics in the maintenance state:

- Hardware diagnostic failures

  Traceability: ARMY, 20 July 1996
  Priority ???

- Hardware diagnostic status

  Traceability: ARMY, 20 July 1996
  Priority ???

- Peripheral diagnostic failures

  Traceability: ARMY, 20 July 1996
  Priority ???

- Peripheral diagnostic status

  Traceability: ARMY, 20 July 1996
  Priority ???